PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 7 : H04L 9/32

A1

(11) Numéro de publication internationale: **WO 00/45549**

(43) Date de publication internationale: 3 août 2000 (03.08.00)

(21) Numéro de la demande internationale: PCT/FR00/00174

(22) Date de dépôt international: 26 janvier 2000 (26.01.00)

(30) Données relatives à la priorité:
99/00887 27 janvier 1999 (27.01.99) FR

(71) Déposant *(pour tous les Etats désignés sauf US)*: FRANCE TELECOM [FR/FR]; 6, Place d'alleray, F–75015 Paris (FR).

(72) Inventeurs; et
(75) Inventeurs/Déposants *(US seulement)*: GIRAULT, Marc [FR/FR]; 9 Rue Bernard Vanier, F–14000 Caen (FR). PAILLES, Jean–Claude [FR/FR]; 4 Rue Des Loisirs, F–14610 Epron (FR).

(74) Mandataire: DU BOISBAUDRY, Dominique; Société De Protection Des Inventions, 3, Rue Du Docteur Lancereaux, F–75008 Paris (FR).

(81) Etats désignés: CA, JP, US, brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Publiée
Avec rapport de recherche internationale.

(54) Title: AUTHENTICATING OR SIGNATURE METHOD WITH REDUCED COMPUTATIONS

(54) Titre: PROCEDE D'AUTHENTIFICATION OU DE SIGNATURE A NOMBRE DE CALCULS REDUIT

(57) Abstract

The invention concerns a method wherein one first entity to be authenticated, having a public key v and a secret key s, said keys being connected by $v=s^t \pmod n$ wherein n is an integer called modulus and t a parameter, and a second authenticating entity, which knows the public key v. Said method comprises zero–knowledge data exchanges between the entity to be authenticated and the authenticating entity and cryptographic computations concerning said data, some of the computations being performed modulo n. The method is characterised in that the modulus n is particular to the authenticated entity, which communicates said modulus to the authenticating entity.

(57) Abrégé

Le procédé met en oeuvre une première entité "à authentifier", possédant une clé publique v et une clé secrète s, ces clés étant reliées par $v=s^{-t} \pmod n$ où n est un entier appelé module et t un paramètre, et une seconde entité "authentifiante", connaissant la clé publique v. Ce procédé comprend des échanges d'informations du type à apport nul de connaissance entre l'entité à authentifier et l'entité authentifiante et des calculs cryptographiques portant sur ces informations, certains calculs étant effectués modulo n. Le procédé de l'invention est caractérisé en ce que le module n est propre à l'entité authentifiée, laquelle communique ce module à l'entité authentifiante

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	**ES**	Espagne	**LS**	Lesotho	**SI**	Slovénie
AM	Arménie	**FI**	Finlande	**LT**	Lituanie	**SK**	Slovaquie
AT	Autriche	**FR**	France	**LU**	Luxembourg	**SN**	Sénégal
AU	Australie	**GA**	Gabon	**LV**	Lettonie	**SZ**	Swaziland
AZ	Azerbaïdjan	**GB**	Royaume-Uni	**MC**	Monaco	**TD**	Tchad
BA	Bosnie-Herzégovine	**GE**	Géorgie	**MD**	République de Moldova	**TG**	Togo
BB	Barbade	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tadjikistan
BE	Belgique	**GN**	Guinée	**MK**	Ex-République yougoslave de Macédoine	**TM**	Turkménistan
BF	Burkina Faso	**GR**	Grèce			**TR**	Turquie
BG	Bulgarie	**HU**	Hongrie	**ML**	Mali	**TT**	Trinité-et-Tobago
BJ	Bénin	**IE**	Irlande	**MN**	Mongolie	**UA**	Ukraine
BR	Brésil	**IL**	Israël	**MR**	Mauritanie	**UG**	Ouganda
BY	Bélarus	**IS**	Islande	**MW**	Malawi	**US**	Etats-Unis d'Amérique
CA	Canada	**IT**	Italie	**MX**	Mexique	**UZ**	Ouzbékistan
CF	République centrafricaine	**JP**	Japon	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Pays-Bas	**YU**	Yougoslavie
CH	Suisse	**KG**	Kirghizistan	**NO**	Norvège	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	République populaire démocratique de Corée	**NZ**	Nouvelle-Zélande		
CM	Cameroun			**PL**	Pologne		
CN	Chine	**KR**	République de Corée	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Roumanie		
CZ	République tchèque	**LC**	Sainte-Lucie	**RU**	Fédération de Russie		
DE	Allemagne	**LI**	Liechtenstein	**SD**	Soudan		
DK	Danemark	**LK**	Sri Lanka	**SE**	Suède		
EE	Estonie	**LR**	Libéria	**SG**	Singapour		

PROCEDE D'AUTHENTIFICATION OU DE SIGNATURE A NOMBRE DE CALCULS REDUIT

Domaine technique

La présente invention a pour objet un procédé d'authentification ou de signature à nombre de calculs réduit.

L'invention concerne plus précisément le domaine de la cryptographie dite à clé publique. Dans de tels procédés, l'entité à authentifier possède une clé secrète et une clé publique associée. L'entité authentifiante a uniquement besoin de cette clé publique pour réaliser l'authentification.

L'invention concerne plus précisément encore le domaine des procédés d'authentification dits à connaissance nulle ou sans apport de connaissance ("zero-knowledge"). Dans ce type de procédé, l'authentification se déroule suivant un protocole qui, de façon prouvée, et sous des hypothèses reconnues comme parfaitement raisonnables par la communauté scientifique, ne révèle rien sur la clé secrète de l'entité à authentifier.

Plus précisément encore, l'invention concerne des procédés sans apport de connaissance basés sur le problème de la factorisation (c'est-à-dire sur la difficulté de décomposer de grands entiers en un produit de nombres premiers).

L'invention trouve une application dans tous les systèmes nécessitant d'authentifier des entités ou des messages, ou de signer des messages, et plus particulièrement dans les systèmes où le nombre de calculs effectués par l'entité authentifiée constitue un paramètre critique. C'est notamment le cas des

cartes à microcircuit standards ou à bas coût, non pourvues d'un coprocesseur arithmétique (appelé souvent cryptoprocesseur) pour accélérer les calculs cryptographiques.

Une application typique de l'invention est le porte-monnaie électronique, qui requiert un très haut niveau de sécurité, tout en excluant l'usage d'un cryptoprocesseur, soit pour des raisons de coût, soit pour des raisons techniques (par exemple l'utilisation d'une interface sans contact), soit pour les deux.

Une autre application possible est la télécarte de future génération, pour laquelle les contraintes de coût sont encore bien plus sévères que pour le porte-monnaie électronique.

Etat de la technique antérieure

De nombreux protocoles d'identification du type sans apport de connaissance sont connus. On peut citer, par exemple :

- le protocole de FIAT-SHAMIR décrit dans l'article de A. FIAT et A. SHAMIR intitulé "How to prove yourself : Practical solutions to identification and signature problems", publié dans "Advances in Cryptology : Proceedings of CRYPTO'86, Lecture Notes in Computer Science", vol. 263, Springer-Verlag, Berlin, 1987, pp. 186-194,
- le protocole de GUILLOU-QUISQUATER décrit dans l'article de L.C. GUILLOU et J.J. QUISQUATER, intitulé "A practical zero-knowledge protocole fitted to security microprocessors minimizing both transmission and memory", publié dans "Advances in Cryptology : Proceedings of EUROCRYPT'88, Lecture

Notes in Computer Science", vol. 330, Springer-verlag, Berlin, 1988, pp. 123-128,

- le protocole de GIRAULT décrit dans la demande de brevet français FR-A-2 716 058, basé sur le problème dit du logarithme discret.

De façon générale, la plupart des protocoles d'identification (ou d'authentification de message) à apport nul de connaissance se déroulent en trois échanges. On supposera, afin de simplifier la description, que l'entité authentifiante B connaît déjà tous les paramètres publics caractéristiques de l'entité à authentifier A, à savoir son identité, sa clé publique, etc..

Lors du premier échange, A fournit à B une valeur c dite "engagement", image par une fonction pseudo-aléatoire h d'un paramètre x (lui-même calculé à partir d'un nombre r choisi au hasard par A), ainsi que, s'il y a lieu, du message à authentifier ou à signer : $c=h(x,[M])$ où la notation [M] exprime que M est optionnel. C'est la première étape. Dans certains protocoles, il peut y avoir plusieurs engagements.

Lors d'un deuxième échange, B envoie à A un paramètre e choisi au hasard (la "question"). C'est la deuxième étape.

Lors du troisième échange, A fournit à B une "réponse" y, cohérente avec la question e, l'engagement c et la clé secrète v de A (troisième étape).

Enfin, B contrôle la réponse reçue. Plus précisément, B recalcule x à partir des éléments y, e et v par $x=\varphi(y,e,v)$; puis il vérifie que : $c=h(\varphi(v,e,y),[M])$ (quatrième étape).

Dans le cas où il n'y a pas de message à authentifier, le recours à la fonction pseudo-aléatoire

h est optionnel. On peut prendre alors c=x. La vérification consiste alors à vérifier que $x=\varphi(y,e,v)$.

Dans certains protocoles, il y a un ou deux échanges supplémentaires entre les entités à authentifier et authentifiante.

Dans le cas d'une signature de message, les deux premiers échanges sont supprimés, car le paramètre e est choisi égal à c ; A calcule alors successivement, et seul, c, e(=c) et y.

Le nombre u de questions possibles est directement relié au niveau de sécurité du protocole. Ce dernier est défini comme la probabilité p de détection d'un imposteur (c'est-à-dire d'une entité C qui tente frauduleusement de se faire passer pour A), et est caractérisé par un paramètre k. Les nombres p et k sont reliés par l'égalité : $p=1-2^{-k}$. En d'autres termes, l'imposteur n'a qu'une chance sur 2^k de réussir son imposture. Dans le cas présent, on peut montrer que, si le protocole repose sur un problème mathématique difficile, et si les engagements sont de longueur suffisante, alors il suffit que la longueur de u soit égale à k bits. Typiquement, k est égal à 32 bits, ce qui donne seulement une chance sur quatre milliards de réussir une imposture. Dans les applications où l'échec d'une identification peut avoir des conséquences très néfastes (poursuite judiciaire par exemple), cette longueur peut être réduite à quelques bits.

Dans les protocoles basés sur la factorisation, le calcul de x à partir de r, ou le calcul de y à partir de e, ou les deux, implique(nt) des opérations modulo n où n est un nombre composé difficile à factoriser. Ce nombre est de type universel, c'est-à-

dire généré par une tierce partie de confiance, mémorisé et utilisé par toutes les entités qui y sont rattachées. Le caractère universel de n implique qu'il est de très grande taille (typiquement 1024 bits), car la découverte de la factorisation de n compromettrait les clés secrètes de tous les utilisateurs.

Dans leur version de base, aucun des protocoles mentionnés plus haut ne peut être mis en oeuvre dans une application soumise à de fortes contraintes, (bas coût, faible complexité) telles que décrites dans la section précédente, car les calculs requis ne pourraient être effectués par une carte à microcircuit qui ne serait pas dotée d'un cryptoprocesseur.

La demande de brevet français FR-A-2 752 122 décrit bien une optimisation de ces protocoles, mais cette optimisation reste limitée aux protocoles basés sur le logarithme discret dans un mode dit "à précalculs" qui présente l'inconvénient d'impliquer des rechargements à intervalles réguliers.

La présente invention a justement pour but de remédier à cet inconvénient. Elle tend à réduire le nombre de calculs effectués par l'entité authentifiée dans les protocoles d'identification (ou d'authentification de message ou de signature de message) sans apport de connaissance basés sur la factorisation, cette réduction pouvant atteindre un facteur 2 ou 3.

Elle rend ainsi possible, et plus particulièrement quand on la couple avec le protocole Guillou-Quisquater, l'exécution rapide d'un algorithme d'identification (ou d'authentification de message ou de signature de message) à clé publique dans une carte

à microcircuit standard à bas coût, pour des applications telles que le porte-monnaie électronique ou la télécarte de future génération.

Exposé de l'invention

Ce but est atteint en choisissant pour le module n non pas un paramètre de type universel, mais un paramètre de type individuel (en d'autres termes, chaque utilisateur possède sa propre valeur de n), et d'exploiter ce choix des deux manières suivantes, (qui peuvent d'ailleurs être avantageusement combinées) :

1) d'abord en choisissant une taille de n inférieure à la valeur usuelle (typiquement inférieure à 1000 et par exemple comprise entre 700 et 800) ; cela est possible car la découverte de la factorisation de n ne compromet plus que la clé secrète de l'utilisateur correspondant et en aucune façon celle des autres ; cette seule modification permet de réduire déjà d'environ 40% la durée des calculs effectués modulo n ;
2) si l'utilisateur a conservé les facteurs premiers de n dans la mémoire de son dispositif de sécurité, on peut mettre en oeuvre la technique dite des restes chinois, pour réduire encore d'environ 40% la durée des calculs effectués modulo n, lorsque le nombre de facteurs premiers est 2 ; cette réduction peut être encore amplifiée en utilisant plusieurs facteurs premiers (typiquement 3 ou 4).

Au total, on peut donc réduire les temps de calcul modulo n d'au moins 60%, c'est-à-dire d'au moins un facteur 2.

De façon précise, l'invention a pour objet un procédé d'authentification mettant en oeuvre une première entité dite "à authentifier", possédant une clé publique v et une clé secrète s, ces clés étant reliées par une opération modulo n où n est un entier appelé module, et une seconde entité dite "authentifiante", connaissant la clé publique v, ces entités comprenant des moyens aptes à échanger des informations du type à apport nul de connaissance et à effectuer des calculs cryptographiques portant sur ces informations, certains calculs étant effectués modulo n, ce procédé étant caractérisé en ce que le module n est propre à l'entité à authentifier, laquelle communique ce module à l'entité authentifiante.

Les entités dont il est question peuvent être, par exemple des cartes à microcircuit, des porte-monnaie électroniques, des télécartes, etc ...

Dans un mode de mise en oeuvre avantageux, l'opération modulo n est du type $v=s^{-t}$ (mod n) où t est un paramètre, et les échanges d'informations du type à apport nul de connaissance et les calculs cryptographiques sont les suivants :

- l'entité à authentifier choisit au hasard un (des) nombre(s) entier(s) r compris entre 1 et n-1 et calcule un (des) paramètre(s) x égal (égaux) à r^t(mod n), puis un (des) nombre(s) c appelé(s) engagement(s) qui est (sont) une (des) fonction(s) de ce (ces) paramètre(s) et éventuellement d'un message (M), et envoie cet (ces) engagement(s) à l'entité authentifiante ;
- l'entité authentifiante reçoit le ou les engagement(s) c, choisit au hasard un nombre e

appelé "question" et envoie cette question à l'entité à authentifier ;

- l'entité à authentifier reçoit la question e, effectue un (des) calcul(s) utilisant cette question e et la clé secrète s, le résultat de ce (ces) calcul(s) constituant une (des) réponse(s) y, et envoie cette (ces) réponse(s) à l'entité authentifiante ;
- l'entité authentifiante reçoit la (les) réponse(s) y, effectue un calcul utilisant la clé publique v et le module n, et vérifie par une opération modulo n que le résultat de ce calcul est bien cohérent avec le (les) engagement(s) reçu(s).

La taille du nombre n, exprimée en nombre de bits, est inférieure à 1000. Elle peut être, par exemple, comprise entre 700 et 800.

La présente invention a également pour objet un procédé de signature de message par une entité dite "signataire", cette entité possédant une clé publique v et une clé secrète s, ces clés étant reliées par une opération modulo n où n est un entier appelé "module" et t un paramètre, procédé dans lequel l'entité signataire calcule un engagement c fonction notamment du message à signer et un nombre y fonction de la clé secrète, émet les nombres y et c qui constituent la signature du message et le message, ce procédé étant caractérisé en ce que le module n est propre au signataire.

Dans un mode de mise en oeuvre avantageux, le signataire choisit au hasard un nombre entier r compris entre 1 et n-1, calcule un paramètre x égal à

$r^t \pmod n$, calcule un nombre c fonction du paramètre x et du message à signer, calcule un nombre y à l'aide de sa clé secrète s et fonction des nombres r et e, et émet les nombres c et y comme signature.

Description détaillée de modes particuliers de mise en oeuvre de l'invention

Dans la description qui suit, l'invention est supposée être appliquée au protocole GUILLOU-QUISQUATER mais, naturellement, il ne s'agit là que d'un exemple et l'invention n'est nullement limitée à ce protocole.

On rappelle que dans le protocole de GUILLOU-QUISQUATER, les paramètres universels sont le module n, produits de nombres premiers et comprenant au moins 1024 bits, et un nombre t entier.

La clé publique v et la clé secrète s sont reliées par l'équation : $v=s^{-t} \pmod n$.

Le niveau de sécurité choisi est u (inférieur ou égal à t, et le plus souvent, u=t).

L'authentification de A par B, que l'on peut appeler respectivement Alice et Bob selon la terminologie en usage, se déroule comme suit :

1. Alice choisit r dans l'intervalle [1,n-1], calcule $x=r^t \pmod n$ puis c=h(x,[M]) et envoie c à Bob.
2. Bob choisit e dans l'intervalle [0,u-1] et envoie e à Alice.
3. Alice calcule $y=rs^e \pmod n$ et envoie y à Bob.
4. Bob calcule $x=y^t v^e \pmod n$ et vérifie que c=h(x,[M])

Dans le cas où il n'y a pas de message à authentifier, le recours à la fonction pseudo-aléatoire h est optionnel : on peut prendre c=x. La vérification consiste alors à vérifier que $x=y^t v^e$ (modulo n).

Avec le protocole modifié selon l'invention, le seul paramètre universel est t.

La clé publique est (n,v), où n a au moins 768 bits. La clé publique v et la clé secrète s d'Alice sont reliées par l'équation : $v=s^{-t} \pmod n$.

La clé secrète peut aussi inclure les facteurs premiers de n afin de bénéficier du deuxième volet de l'invention.

Le paramètre t peut être inclus dans la clé publique (dans ce cas, il n'y a plus de paramètre universel).

Le niveau de sécurité choisi par Alice et Bob est u (inférieur ou égal à t ; souvent u=t).

L'authentification d'Alice par Bob se déroule comme décrit plus haut, mais avec des calculs plus rapides grâce à un module plus petit.

Puisque tous les calculs d'Alice sont effectués modulo n, le facteur de gain obtenu sur une unique multiplication modulaire se répercute sur l'ensemble des calculs effectués par Alice durant l'exécution du protocole. Il en serait de même avec les protocoles de Fiat-Shamir ou de Girault par exemple (dans ce dernier cas, il n'y a pas de gain dans l'étape 3 puisqu'il n'y a plus de calculs modulaires, mais de toute façon le temps d'exécution de cette étape est négligeable par rapport à l'exponentiation modulaire de la première étape).

L'invention peut également être mise en oeuvre par la technique dite des restes chinois, qui consiste à effectuer les calculs modulo chacun des nombres premiers composant n. Comme ces nombres sont nécessairement beaucoup plus petits, ces calculs sont

rapides. Il reste à calculer le résultat modulo n à l'aide d'une opération dite de reconstitution. Cette technique est décrite dans l'article de J.J QUISQUATER et C. COUVREUR, intitulé "Fast decipherment algorithm for RSA public-key cryptosystem", publié dans "Electronic Letters", vol. 18, Octobre 1982, pp. 905-907.

On considère donc le cas où n est le produit de deux facteurs premiers p et q.

D'après le théorème de Bezout, il existe deux entiers a et b tels que ap+bq=1.

Pour calculer $y=x^e \pmod n$, on commence par "réduire" x modulo chacun des nombres premiers en calculant $x_p=x \pmod p$ et $x_q=x \pmod q$. On réduit également e modulo (p-1) et (q-1) en calculant $e_p=e \bmod (p-1)$ et $e_q=e \bmod (q-1)$. (Dans le protocole de Guillou-Quisquater, e est toujours inférieur à p-1 et q-1 et par conséquent ep=eq=e).

On calcule alors $y_p=x_p^{e_p} \pmod p$ et $y_q=x_q^{e_q} \pmod q$. Quand p et q sont de tailles semblables, chacun de ces calculs est environ 8 fois plus rapide que le calcul $y=x^e \pmod n$ quand la taille de e est celle de n (premier cas) ; 4 fois plus rapide quand elle est inférieure ou égale à celle de p (deuxième cas comme par exemple dans l'algorithme). L'ensemble des deux calculs est donc, soit 4 fois plus rapide, soit 2 fois plus rapide.

Il reste à reconstituer y à partir de y_p et y_q, ce qui est réalisé par l'opération :

$$y=y_p+ap(y_q-y_p) \pmod n$$

Au total, la méthode des restes chinois permet d'accélérer le calcul d'un facteur compris entre 3 et 4 dans le premier cas, entre 1,5 et 2 dans le deuxième cas. Lorsque le nombre de facteurs premiers (supposés de tailles semblables) est supérieure à 2 et égal à k, le facteur d'accélération est proche de k^2 dans le premier cas, proche de k dans le deuxième cas.

REVENDICATIONS

1. Procédé d'authentification mettant en oeuvre une première entité dite "à authentifier" (A), possédant une clé publique v et une clé secrète s, ces clés étant reliées par une opération modulo n où n est un entier appelé module, et une seconde entité dite "authentifiante" (B), connaissant la clé publique v, ces entités, comprenant des moyens aptes à échanger des informations du type à apport nul de connaissance et à effectuer des calculs cryptographiques portant sur ces informations, certains calculs étant effectués modulo n, ce procédé étant caractérisé en ce que le module n est propre à l'entité à authentifier (A), laquelle communique ce module à l'entité authentifiante (B).

2. Procédé selon la revendication 1, dans lequel l'opération modulo n est du type $v=s^{-t}$ (mod n), t étant un paramètre et les échanges d'informations du type à apport nul de connaissance et les calculs cryptographiques sont les suivants :

- l'entité à authentifier (A) choisit au hasard un (des) nombre(s) entier(s) r compris entre 1 et n-1 et calcule un (des) paramètre(s) (x) égal (égaux) à r^t(mod n), puis un (des) nombre(s) c appelé(s) engagement(s) qui est (sont) une (des) fonction(s) de ce (ces) paramètre(s) et éventuellement d'un message (M), et envoie cet (ces) engagement(s) à l'entité authentifiante (B) ;
- l'entité authentifiante (B) reçoit le ou les engagement(s) c, choisit au hasard un nombre e

appelé "question" et envoie cette question à l'entité à authentifier (A) ;

- l'entité à authentifier (A) reçoit la question e, effectue un (des) calcul(s) utilisant cette question e et la clé secrète s, le résultat de ce (ces) calcul(s) constituant une (des) réponse(s) y, et envoie cette (ces) réponse(s) à l'entité authentifiante (B) ;
- l'entité authentifiante (B) reçoit la (les) réponse(s) y, effectue un calcul utilisant la clé publique v et le module n, et vérifie par une opération modulo n que le résultat de ce calcul est bien cohérent avec le (les) engagement(s) reçu(s).

3. Procédé selon la revendication 2, dans lequel la taille du nombre n, exprimée en nombre de bits, est inférieure à 1 000.

4. Procédé selon la revendication 3, dans lequel la taille du nombre n est comprise entre 700 et 800.

5. Procédé selon l'une quelconque des revendications 1 à 4, dans lequel n est le produit d'au moins deux nombres premiers (p, q) et dans lequel les opérations modulo n sont effectuées par la méthode dite "des restes chinois".

6. Procédé de signature de message par une entité dite "signataire" (A), cette entité possédant une clé publique v et une clé secrète s, ces clés étant reliées par une opération modulo n où n est un entier appelé "module" comprenant des moyens aptes à calculer un

engagement c fonction notamment du message à signer M et un nombre y fonction de la clé secrète, à émettre les nombres y et c qui constituent la signature du message M et le message M, ce procédé étant caractérisé en ce que le module n est propre au signataire.

7. Procédé de signature selon la revendication 6, dans lequel l'opération modulo n est l'opération $v=s^{-t}(\text{mod } n)$ et dans lequel le signataire choisit au hasard un nombre entier r compris entre 1 et n-1, calcule un paramètre x égal à $r^t(\text{mod } n)$, calcule un nombre c fonction du paramètre x et du message à signer M, calcule un nombre y à l'aide de sa clé secrète s et fonction des nombres r et e, et émet les nombres c et y comme signature.

INTERNATIONAL SEARCH REPORT

Inte[redacted]al Application No
PCT/FR 00/00174

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	BRANDT J ET AL: "Zero-knowledge authentication scheme with secret key exchange" ADVANCES IN CRYPTOLOGY - CRYPTO '88. PROCEEDINGS, SANTA BARBARA, CA, USA, 21-25 AUG. 1988, pages 583-588, XP000090662 1990, Berlin, West Germany, Springer-Verlag, West Germany ISBN: 3-540-97196-3 page 584, paragraph 4 --- -/--	1,6

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 February 2000	25/02/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Zucka, G

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 00/00174

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X	FIAT A ET AL: "How to prove yourself: practical solutions to identification and signature problems" ADVANCES IN CRYPTOLOGY - CRYPTO '86 PROCEEDINGS, SANTA BARBARA, CA, USA, 11-15 AUG. 1986, pages 186-194, XP000090668 1987, Berlin, West Germany, Springer-Verlag, West Germany ISBN: 3-540-18047-8 cited in the application page 187 -page 188 ---	1,6
A	KONIGS H -P: "Cryptographic identification methods for smart cards in the process of standardization" IEEE COMMUNICATIONS MAGAZINE, JUNE 1991, USA, vol. 29, no. 6, pages 42-48, XP002126721 ISSN: 0163-6804 page 46, column 2 -page 47, column 2 ---	1-7
A	GUILLOU L C ET AL: "A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory" ADVANCES IN CRYPTOLOGY - EUROCRYPT '88. WORKSHOP ON THE THEORY AND APPLICATION OF CRYPTOGRAPHIC TECHNIQUES. PROCEEDINGS, DAVOS, SWITZERLAND, 25-27 MAY 1988, pages 123-128, XP000562467 1988, Berlin, West Germany, Springer-Verlag, West Germany ISBN: 3-540-50251-3 cited in the application page 125 -page 127 ---	1,6
A	QUISQUATER J -J ET AL: "Fast decipherment algorithm for RSA public-key cryptosystem" ELECTRONICS LETTERS, 14 OCT. 1982, UK, vol. 18, no. 21, pages 905-907, XP000577331 ISSN: 0013-5194 cited in the application figure 1 ---	5
A	FR 2 752 122 A (FRANCE TELECOM) 6 February 1998 (1998-02-06) cited in the application page 6 -page 13 ---	1-7
A	FR 2 716 058 A (FRANCE TELECOM ;POSTE) 11 August 1995 (1995-08-11) cited in the application page 8 -page 13, paragraph 2 -----	1-7

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter[illegible]al Application No
PCT/FR 00/00174

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
FR 2752122 A	06-02-1998	NONE	
FR 2716058 A	11-08-1995	DE 69505703 D	10-12-1998
		DE 69505703 T	02-06-1999
		EP 0666664 A	09-08-1995

RAPPORT DE RECHERCHE INTERNATIONALE

Dem[redacted]ternationale No
PCT/FR 00/00174

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/32

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	BRANDT J ET AL: "Zero-knowledge authentication scheme with secret key exchange" ADVANCES IN CRYPTOLOGY - CRYPTO '88. PROCEEDINGS, SANTA BARBARA, CA, USA, 21-25 AUG. 1988, pages 583-588, XP000090662 1990, Berlin, West Germany, Springer-Verlag, West Germany ISBN: 3-540-97196-3 page 584, alinéa 4 --- -/--	1,6

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquee)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
18 février 2000	25/02/2000

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Zucka, G

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	FIAT A ET AL: "How to prove yourself: practical solutions to identification and signature problems" ADVANCES IN CRYPTOLOGY - CRYPTO '86 PROCEEDINGS, SANTA BARBARA, CA, USA, 11-15 AUG. 1986, pages 186-194, XP000090668 1987, Berlin, West Germany, Springer-Verlag, West Germany ISBN: 3-540-18047-8 cité dans la demande page 187 -page 188	1,6
A	KONIGS H -P: "Cryptographic identification methods for smart cards in the process of standardization" IEEE COMMUNICATIONS MAGAZINE, JUNE 1991, USA, vol. 29, no. 6, pages 42-48, XP002126721 ISSN: 0163-6804 page 46, colonne 2 -page 47, colonne 2	1-7
A	GUILLOU L C ET AL: "A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory" ADVANCES IN CRYPTOLOGY - EUROCRYPT '88. WORKSHOP ON THE THEORY AND APPLICATION OF CRYPTOGRAPHIC TECHNIQUES. PROCEEDINGS, DAVOS, SWITZERLAND, 25-27 MAY 1988, pages 123-128, XP000562467 1988, Berlin, West Germany, Springer-Verlag, West Germany ISBN: 3-540-50251-3 cité dans la demande page 125 -page 127	1,6
A	QUISQUATER J -J ET AL: "Fast decipherment algorithm for RSA public-key cryptosystem" ELECTRONICS LETTERS, 14 OCT. 1982, UK, vol. 18, no. 21, pages 905-907, XP000577331 ISSN: 0013-5194 cité dans la demande figure 1	5
A	FR 2 752 122 A (FRANCE TELECOM) 6 février 1998 (1998-02-06) cité dans la demande page 6 -page 13	1-7
A	FR 2 716 058 A (FRANCE TELECOM ;POSTE) 11 août 1995 (1995-08-11) cité dans la demande page 8 -page 13, alinéa 2	1-7

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No
PCT/FR 00/00174

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
FR 2752122 A	06-02-1998	AUCUN	
FR 2716058 A	11-08-1995	DE 69505703 D	10-12-1998
		DE 69505703 T	02-06-1999
		EP 0666664 A	09-08-1995